

疫情下的数据利用和个人信息保护再权衡

张郁安

(中国信息通信研究院政策与经济研究所, 北京 100191)

摘要:在新冠肺炎疫情抗击中,大数据的利用为抗击疫情提供了有力武器,同时也凸显了在公共突发事件下如何权衡公共需要与个人信息保护这一重要问题。目前我国已经基本建立了公共突发事件下的信息利用规则,赋予政府部门广泛的信息收集、利用职责,但相关规则与个人信息保护制度的协调性不足。建议加强对公共突发事件下的数据利用与个人信息保护再权衡,细化相关场景下的数据利用具体规则。

关键词:数据利用;个人信息保护;突发事件

中图分类号:D923

文献标识码:A

引用格式:张郁安. 疫情下的数据利用和个人信息保护再权衡[J]. 信息通信技术与政策, 2021,47(1): 53-56.

doi: 10. 12267/j. issn. 2096-5931. 2021. 01. 011

0 引言

全国范围的新冠肺炎疫情抗击工作开展以来,围绕“早发现、早隔离”的防治原则,人们利用包括大数据技术在内的多种手段,进行重点人群的监测预警、统计分析,以准确、及时、全面的信息为武器对抗疫情。相关的应用包括实时监测车辆、人口动态信息,或利用大数据开展人员流动监测,为研判疫情态势提供技术支持;包括面向公众的“同程排查”服务,用户输入行程日期、车次和地区,即可查询已被披露的新冠肺炎确诊患者同行的火车、飞机和地铁等等。北京、天津、江苏等地方主管部门公布“病例发病期间活动过的小区或场所”,帮助市民及时了解疾病线索,便于社区有针对性地开展疫情防控工作。除此以外,社会上也出现过一些明显违法或失范的信息利用活动,比如在微信群中公开、转发有武汉接触史人员的姓名、身份证号、行程、位置等个人信息。面对公共卫生突发事件,在种种信息利用活动面前,如何权衡公共需要与个人权利,以划定合理的信息保护与利用的界限显得愈发重要。

1 我国公共卫生突发事件下的信息利用和保护规则

信息的收集、利用对于传染病疫情防控的重要意义不言而喻,当前我国已基本建立起疫情下的个人信息收集与利用规则框架,通过《突发事件应对法》《传染病防治法》《突发公共卫生事件应急条例》,结合《网络安全法》的相关规定,从应急保障、信息公开、信息保护等角度,分别对政府部门、企业组织以及个人在传染病疫情防控场景下的责任义务进行了规定,为疫情下相关信息的合理利用提供了基本准则。

1.1 政府部门按照法定职责收集、公布事件相关信息,对疫情开展监测

政府及有关部门、专业机构应当“通过多种途径收集突发事件信息”(《突发事件应对法》第三十八条)。政府应当主动公开“突发公共事件的应急预案、预警信息及应对情况”(《政府信息公开条例》第二十条)。卫生行政主管部门负责向社会发布突发公共卫生事件的信息(《突发公共卫生事件应急条例》第二十五条)。除了收集和发布疫情事件信息以外,卫生行政部门和

相关政府部门还应当开展监测预警。有关部门、医疗卫生机构应当对传染病做到“早发现、早报告、早隔离”(《突发公共卫生事件应急条例》第四十二条)。各级人民政府应当开展“流动人口管理”,落实预防、控制措施,非事件发生地区也要开展“重点人群、重点场所和重点环节的监测和预防控制工作,防患于未然”(《国家突发公共卫生事件应急预案》,2006年实施)。

在传染病疫情防控中,“突发事件信息”、“预警信息”均可以理解为包括传染病病人、疑似传染病病人、密切接触者等重点人群的健康状况、行踪、位置、工作单位等个人信息。开展“流动人口管理”、“重点人群、重点场所和重点环节的监测和预防控制工作”也将不可避免地涉及大量个人信息收集、分析和利用活动。法律法规赋予政府及有关部门在疫情防控中对个人信息广泛的收集利用权力。底线是不得“故意泄露传染病病人、病原携带者、疑似传染病病人、密切接触者涉及个人隐私的有关信息、资料”(《传染病防治法》第六十八条)。“医疗卫生人员未经当事人同意,不得将传染病病人及其家属的姓名、住址和个人病史以任何形式向社会公开”(《突发公共卫生事件与传染病疫情监测信息报告管理办法》,卫疾控发[2006]332号,第十四条)。

1.2 企业、组织和个人承担信息报告义务,并可利用所掌握的数据支持疫情防控

获悉突发事件信息的公民、法人或者其他组织,应当“立即向所在地人民政府、有关主管部门或者指定的专业机构报告”(《突发事件应对法》第三十八条)。“任何单位和个人发现传染病病人或者疑似传染病病人时,应当及时向附近的疾病预防控制机构或者医疗机构报告”(《传染病防治法》第三十一条)。

《网络安全法》等法律法规对于网络运营者的个人信息保护义务进行了明确界定,包括信息收集的最小化和必要原则,用户知情权,用户同意权,以及对于与第三方(非主管部门)共享的限制等核心规则。

结合前述突发事件管理和传染病防治的有关规定,可以将企业、组织等主体在疫情中处理个人信息及相应的数据保护义务分为3种情况:一是直接发现和疫情相关的信息应当主动向主管部门报告,不受个人信息保护规则的限制。二是按照主管部门要求,或受其委托对用户数据开展分析、利用、研究,辅助疫情防

控工作的,应当按照要求或委托的内容进行数据处理,不能超过主管部门的相关职责权限,同时不受常态下个人信息保护规则的限制。三是自主对用户数据进行分析、利用,用于开发疫情防控相关产品和服务的,应当履行常态下的个人信息保护义务。企业或组织在疫情与常态下的个人信息保护义务对比详情如表1所示。

表1 企业或组织在疫情与常态下的个人信息保护义务对比

状态	最小化和必要原则	用户知情同意	第三方共享限制
疫情	直接发现	×	×
	受委托的数据利用	×	×
	自主的数据利用	√	√
常态	自主的数据利用	√	√

2 域外公共卫生突发事件下的信息保护豁免

将视线投向域外,欧盟、美国等数据保护与利用规则较为发达的国家和地区,均在立法或判例中确立了公共事件中的个人信息处理规则,主要内容包含以下几方面。

2.1 为保护公共利益在一定程度上限制个人信息知情同意权

欧盟《一般数据保护条例》确立了一般情况下的数据主体知情同意原则,但同时也规定了6类无需获得数据主体同意即可处理个人信息的理由。具体包括为保护数据主体及其他自然人的重要利益而处理个人数据,为公共利益而执行任务,或数据控制者被赋予公共职能时必须处理个人数据等。美国《健康保险携带和责任法案》(简称HIPAA)规定在12类涉及“国家利益优先”的情形下,可以不经个人同意而披露及使用健康信息,其中包括公共卫生事件、卫生监管活动、降低卫生或安全风险、重要政府工作等。HIPAA规制的“可识别个人健康信息”同时涵盖了个体信息和集合信息,既包括个人过去、现在和未来的身体和精神健康

信息,相关支付信息,也包括人口学统计数据。

2.2 运用“第三方准则”保护第三方机构向主管部门提供数据或数据分析结果

“第三方原则”是指第三方机构(如医院、电信运营商、保险公司等)应政府部门要求提供其掌握的个人信息,不受美国宪法第四修正案(公民免受无理由搜查和扣押)的限制。该原则是美国法院在处理数据协助义务案件中所应用的一项规则,也适用于强制上报健康数据等活动,数据收集方可以在不经用户同意的情况下变更收集时告知用户的使用目的,并将数据一次性或持续性披露给政府部门。

随着掌握海量用户数据的数字平台兴起,数据用于公益目的的场景将越来越丰富。以防治流感为例,目前美国已经有众多基于用户数据的平台正积极利用贫困、失业、低学历、住房不稳定以及粮食不安全等信息确定高风险人群,以这些数据为基础,帮助医疗行业更准确地预测流感的发病率和入院率,促进医疗资源的有效分配。第三方准则为海量数据用于执法和公益目的搭建了一种框架,值得重视。

2.3 运用比例原则衡量特殊情况下信息利用与保护的合理界限

无论是公共利益优先还是“第三方准则”,都是在利益冲突场景下为权衡信息利用与保护而提出的法律原则,并未解决现实情况下如何划定具体边界的问题。如何在不同场景下在两者之间进行再权衡,很大程度上将取决于比例原则,即将公共需要或公共利益与个人信息受到克减的程度相比较,找到一个相对合理的平衡点。

大数据利用是利益冲突的典型场景,近年来受到各方关注。2013年,美国研究人员Rubinstein在其发表的论文中指出,大数据给隐私保护法带来了挑战:一方面模糊了个人信息和非个人信息的边界,另一方面冲击了信息最小化原则和知情同意原则^[4]。健康或医疗大数据就是这样一个例子,健康信息普遍被认为是最具有个人和秘密特性的信息,但同时也是对识别犯罪嫌疑人、调查流行病、制定公共政策、开展生物医学和行为学研究等具有高度价值的信息。今后在健康大数据领域势必将产生更加多样的数据应用,个人信息利用与保护的界限划定将面临更多挑战。

3 结束语

疫情下的数据利用与个人信息保护实践为完善个人信息保护制度提供了新的观察视角,在数据管理制度不断健全完善的当下具有特别意义,建议政策制定者加强研究,将平衡原则从抽象空洞的基本原则发展为鲜活具体的可操作规范。具体来说可从两方面入手:一方面要不断审视数据利用与个人信息保护的平衡。近年来,我国积极推进个人信息保护的立法和实践,个人信息保护制度不断完善,重点领域的执法力度明显加强。信息保护固然是数字经济时代的应有之义,数据利用则更是社会各领域发展前进的强劲动力,必须在其中维持微妙的平衡。相关部门在规范制定和执行中应开展“平衡性测试”,统筹考虑个人信息的敏感性、个人权益的可恢复性、公共需要的重要性紧迫性等因素,处理好数据管理的“宽”与“严”的关系。另一方面要细化公共事件等特殊场景下的数据利用规则。可以考虑按照数据的不同识别程度,如匿名性、可关联性、可识别性,结合数据的敏感性、重要性、公共需求的迫切性等维度,分别规定不同的利用规则、认定标准、保护措施、管理体制、主体责任。政策制定者应持续发布指导事例,阐释具体个案中不同行业背景下的国家利益、公共利益的具体含义,明确个人信息权利与公共需求、执法协助、学术研究等法律保护事由的合理界限,为数据利用和保护的平衡提供清晰的指引和合理的预期。

参考文献

- [1] Lawrence O. Gostin. Healthy information privacy [J]. Cornell L. Rev, 1995, 80: 454-459.
- [2] Wendy K. Mariner. Reconsidering constitutional protection for health information privacy [J]. U. Pa. J. Const, 2016, 18: 980-990.
- [3] Michael Birnhack. The problem of the orizing privacy: a process-based approach to informational privacy and the case of big medical data [J]. Theoretical Inq, 2019, 20: 265-268.
- [4] Ira S. Rubinstein. Big data: the end of privacy or a new beginning? [J]. Social Science Electronic Publishing, 2013, 3(2): 74-87.

- [5] 中国信息通信研究院. 大数据白皮书[R], 2019.
- [6] 中国信息通信研究院. 数字经济治理白皮书[R], 2019.
- [7] 中国信息通信研究院. 互联网平台治理研究报告[R], 2019.

作者简介:

张郁安 中国信息通信研究院政策与经济研究所工程师,主要从事跨境数据流动、互联网治理、数据治理规则等研究工作

Rebalance of the data process and personal data protection in the epidemic situation

ZHANG Yu'an

(Policy and Economics Research Institute, China Academy of Information and Communications Technology ,
Beijing 100191, China)

Abstract: In the fight against COVID-19, processing of big data is of great use in the dealing of the emergency , which also forth the question of how to rebalance the data process and personal data protection. Although the administrative branch is entitled with a broad power of collecting and analyzing information, there exists still incompetence in the relevant rules. The data process and personal data protection should be rebalanced under the emergency of epidemic situation with specific and detailed rules.

Keywords: data process; personal data protection; public emergency

(收稿日期:2020- 12- 17)